

Risk Driven Outcome-Based Command and Control (C2) Assessment

Michael S. McBeth*

Communication Systems Department
Space and Naval Warfare Systems Center, Charleston
Joint C4ISR Battle Center
116 Lakeview Parkway, Suite 150
Suffolk, VA 23435-2697
(757) 638 4041 Voice
mcbethm@spawar.navy.mil

Abstract

This paper outlines an analysis approach that combines risk assessment, systems dynamics modeling, end-to-end testing, and fine-grained linked simulations to surface deficiencies and identify enhancements for Joint Task Force (JTF) Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) architectures. Conventional wisdom calls for building architecture framework products and executable simulations to understand and assess architecture behavior and performance. Unfortunately, in many cases these framework products do not exist and creating products for an architecture as large as a JTF before deployment is not realistic. The Joint C4ISR Outcome Based Integrated Architecture Assessment (JCOBIAA) team is pursuing an outcome based approach that uses risk assessment and systems dynamics modeling to prioritize issues and reduce the scope of the integrated architecture to be analyzed. The concept of functional threads for task accomplishment is used as a mechanism for analysis. In addition, end-to-end testing is proposed as a technique to address problem areas like interface compatibility and message exchanges since configuring actual hardware and software components in a distributed test environment can be easier and more reliable than developing or employing digital simulations.

1. Introduction

In today's dynamic and global environment, elements of the four Armed Services are often assembled for U.S. Military operations. Unified direction is normally accomplished by establishing a joint force, assigning a mission or objective to the Joint Force Commander (JFC), assigning or attaching appropriate forces to the joint force, and empowering the JFC with sufficient authority over the forces to accomplish the assigned mission. [JCS, 1997].

The Joint Task Force (JTF) Joint Force Commander (JFC) must pull together disparate organizations and their underlying infrastructures to form a cohesive force. The JFC's staff uses Joint instructions and experience learned from previous JTFs to guide this effort. However, each JTF is different—it is built from the resources available at the time to deal with the particular mission at hand. The JFC needs to assess the fitness of the resulting architecture. The reality is that JTFs are formed rapidly with limited time available for assessing and enhancing the

* The author would like to acknowledge the JCOBIAA Team at the Joint C4ISR Battle Center and MITRE. This research represents the views of the author and is not intended to reflect official opinions of the Department of Defense, Joint Forces Command, Department of the Navy, Space and Naval Warfare Systems Center Charleston, or MITRE.

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 2000		2. REPORT TYPE		3. DATES COVERED 00-00-2000 to 00-00-2000	
4. TITLE AND SUBTITLE Risk Driven Outcome-Based Command and Control (C2) Assessment				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Space and Naval Warfare Systems Center, Charleston, Joint C4ISR Battle Center, 116 Lakeview Parkway, Suite 150, Suffolk, VA, 23435-2697				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 23	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

resulting JTF architecture [Ellis, 1999]. Evaluating the performance of architectures by linking specific tasks to individual C4ISR systems, processes, and organizations requires representing all the detailed processes involved. This could include tasks such as the transmission of communications across the battlefield, assessing the impact of logistics on decision making, generating weapon fire control orders, and many others. Although tools continue to evolve, modeling an entire JTF architecture at such a fine grain level takes too long for a rapid assessment of a JTF architecture.

The NATO Code of Best Practice (COBP) for Command and Control (C2) assessment provides an evaluation framework and guidance for conducting C2 assessments [NATO, 1998]. The COBP identifies a technique called “scanning the scenario space” using very fast running systems dynamics models as a prefiltering technique to identify “interesting” segments of the solution space to explore further with fine-grain tools [Starr, 1998].

The alternative approach proposed in this paper is to first use a risk assessment tool to identify potential problem areas so that later modeling and test activities can be focused where they will have the most impact on improving the JTF architecture.

The concept of using risk to guide outcome-based C4ISR assessments grew out of ongoing work at the Joint C4ISR Battle Center (JBC) in Suffolk, Virginia and at the Space and Naval Warfare (SPAWAR) Systems Center in Charleston, South Carolina (SSC-C). At the JBC, the Joint C4ISR Outcome-Based Integrated Architecture Assessment (JCOBIAA) study team is involved in examining and validating efficient JTF C4ISR architecture assessment methodologies. One such methodology developed at SSC-C employs the Joint Maritime Tool for Interoperability Risk Assessment (JMTIRA). JMTIRA is currently used to focus Naval Battlegroup end-to-end interoperability testing efforts on high-risk systems and interfaces. Discovering ways to efficiently prioritize portions of the JTF architecture for detailed analysis may provide the JTF commander with a method to mitigate many of the problems that result from the rapid formation of these complex command and control organizations.

This paper begins with a brief overview of some Joint Task Force basics including organization, phases, and planning. Then the JTF problem is outlined along with some of the challenges associated with integrated architectures. Next, executable architectures and simulations are discussed. This is followed with a discussion of each of the elements of the emerging JCOBIAA methodology. The paper concludes with some comments on challenges yet to be overcome and the future direction of this effort.

2. Background

2.1 Joint Task Force Organization

The JFC determines the command relationship between components and their forces. For example, the Joint Force Land Component Commander (JFLCC) is responsible for planning and executing the ground campaign portion of the overall JTF operation. The role of each component commander in a joint force merits special attention. Component commanders are required to orchestrate the activity of their own forces, branches, and warfare communities. In

addition, they must understand how their force integrates into the overall force structure to best support the JFC's plans and goals. [JCS, 1995]

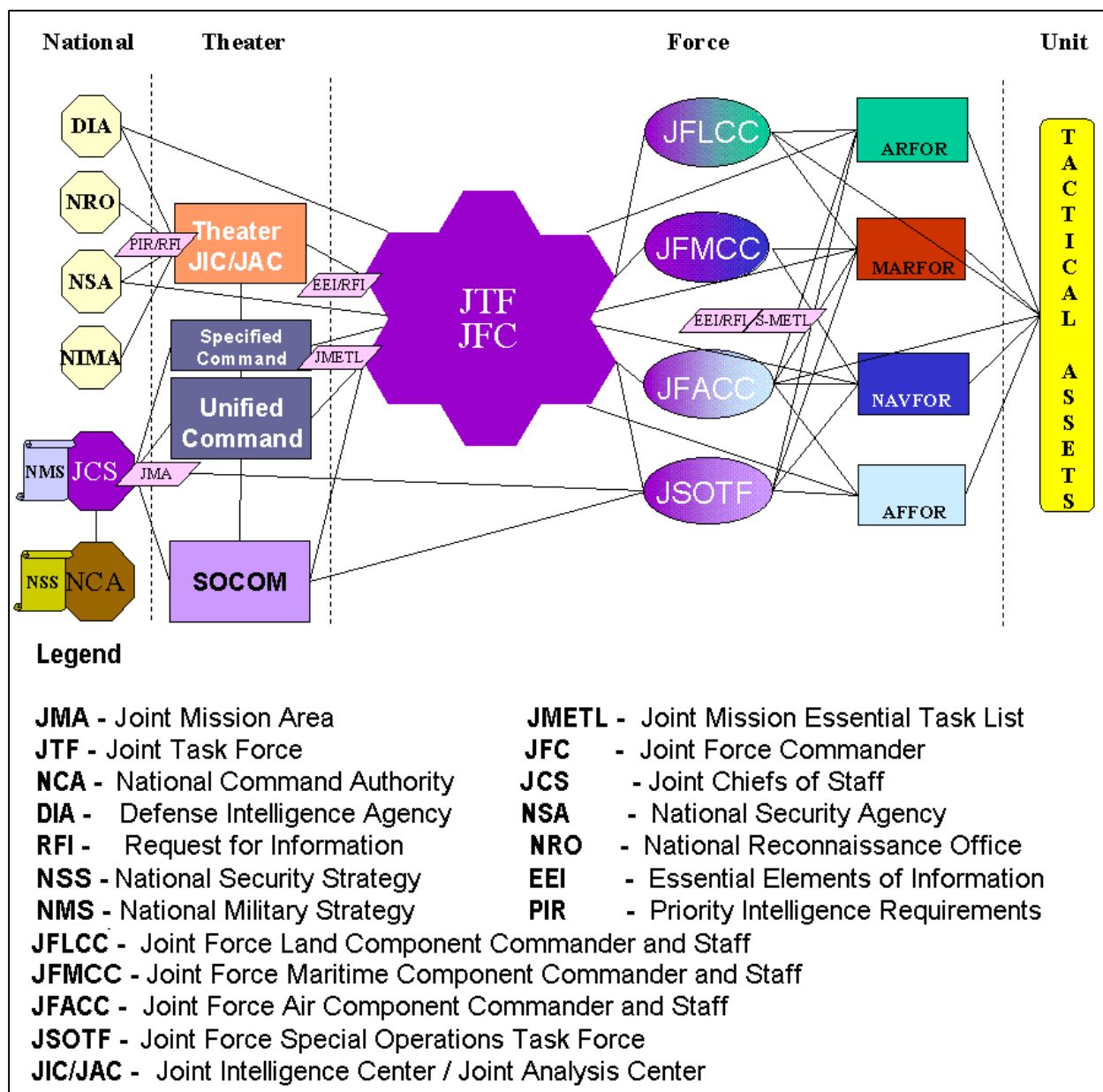


Figure 1. Operational View of a Notional Joint Task Force

Figure 1 shows an operational view of a notional JTF organized from the national, theater, force, and unit perspective. JTFs can be enormous—Desert Storm included over 500,000 troops along with their supporting communications and weapon systems. The resulting military operational organization generates a complex communication architecture with many interfaces and interactions which need to be described from multiple perspectives to gain an understanding of the overall architecture's performance and the expected impact on military operations.

2.2 The Problem

A Joint Task Force is configured for its assigned mission and area of operations. The organizational units, C4ISR systems, and coalition partners can differ from one JTF to the next. The staff responsible for planning and implementing a JTF's C4ISR architecture needs to be able to evaluate the architecture being developed, surface deficiencies and identify solutions in advance of deployment. Figure 2 shows pictorially the problem facing the JTF Commander.

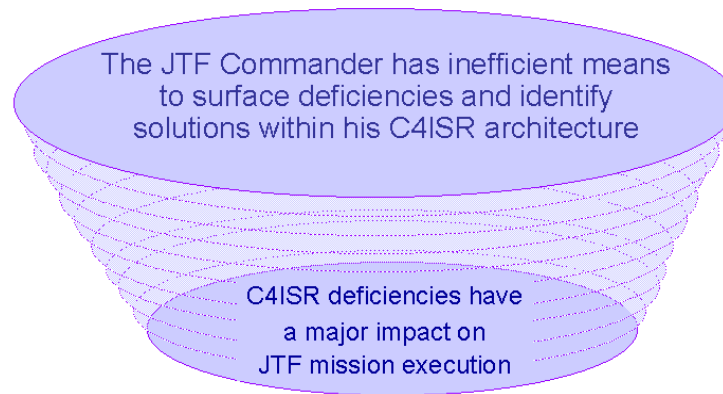


Figure 2. Problem Statement.

2.3 JCOBIAA Methodology

The JCOBIAA methodology is being developed to address the architecture assessment problem and reduce interoperability problems that are usually not discovered until the architecture is fielded or deployed to remote locations. The basis of the methodology is to use a risk assessment tool to identify the highest priority or critical aspects of the JTF architecture and employ detailed modeling and simulation tools or actual hardware and software testing to further examine risk and identify risk mitigation procedures. Ideally, the mature JCOBIAA methodology will enable early assessment and reduce interoperability failures in the field. This would primarily be conducted during the planning stages of JTF operations.

2.4 Joint Task Force Planning

“Deliberate” and “Crisis Action” are typical qualifiers of the process involved in conducting JTF planning and are depicted in Figure 3. The limited amount of time available for crisis action planning is the major difference between the two paths. The planning phases that are impacted by the concurrent architecture design process and the architecture assessment approach are also depicted. The JCOBIAA methodology focuses on planning phases IV and later as shown in Figure 3.

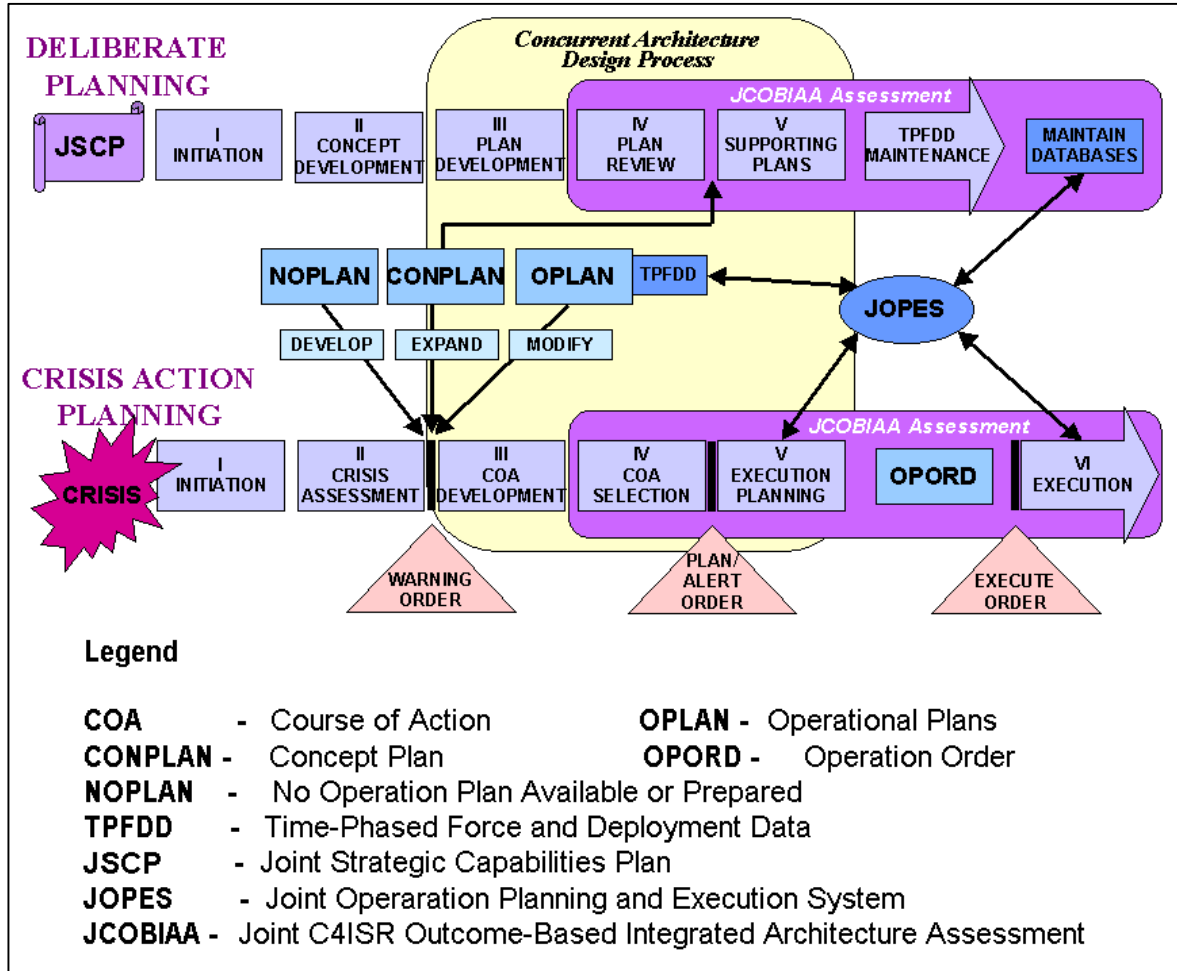


Figure 3. Joint Planning Summary.

2.5 Integrated Architecture Challenge

The Department of Defense (DoD) describes various aspects of the architecture using the concept of architecture views. Three views of a single architecture are specified—the Operational, Systems, and Technical. The operational view describes the required information exchanges to and from elements of the military organizations. In short, it describes who talks to whom and what information is passed between them. The systems view describes the systems employed and the connections required in accordance with the military organizations specified in the operational view. Finally, the technical view describes the minimal set of standards and rules governing the implementation, arrangement, interaction, and interdependence of system elements. The technical view facilitates increased interoperability and promotes efficiency. [CAWG 1997].

Integrated architectures describe the single JTF design using these multiple views. Integrated architectures provide opportunities and challenges to improve mission execution. There is a functional challenge of how to array operational military personnel and staff organizations to make the best use of the architecture to accomplish the mission. There is the design challenge of how to specify the architecture so there is concordance between the views. There is the assessment challenge of how to determine the utility of a given architectural solution in terms of measures of performance, effectiveness, and force effectiveness. [CAWG, 1997]

2.6 Executable Architectures and Simulations

The dynamics of a given real world situation add new dimensions to the challenge of architecture assessment. Understanding and studying the behavior of architectures is greatly enhanced by having an executable model. The term “executable” refers to a model that contains the behaviors inherent in the functional, physical, dynamics, and organizational information drawn from the real world architecture that is modeled. In the planning of a new architecture, notional information can be assimilated from similar existing instantiations. The C4ISR Architecture Framework products provide a description of the static architecture. An executable model is based on the functional model and contains information from rule, data, and dynamic models. See Figure 4. [Levis, 2000]

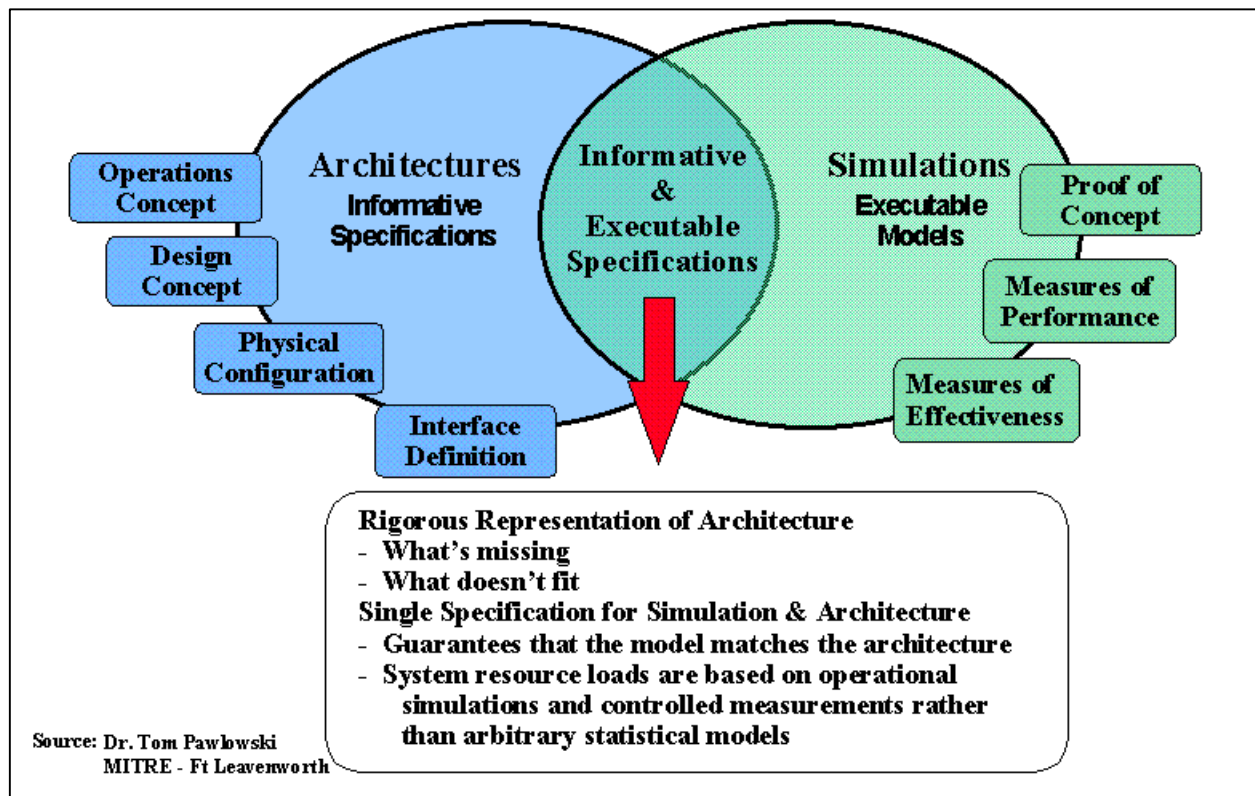


Figure 4. Relationship Between Architectures and Simulations

3. Emerging Methodology

3.1 Overview

The risk assessment methodology proposed for JCOBIAA uses a risk assessment tool along with system dynamic, fine-grained linked models, and end-to-end testing to assess the JTF commander's architecture. The risk assessment tool identifies high-risk areas that need to be examined in more detail. The objective is to suggest solutions to problems prior to the architecture being deployed thus saving time and expense.

A pictorial view of the JCOBIAA methodology is shown in Figure 5. The process begins as an actual joint architecture is being formed. An interoperability risk assessment is conducted by encoding information on the organization, systems, interfaces, and test history into the risk assessment model. Next, functional threads are identified and risk factors are calculated. The risk assessment tool identifies high risk areas in the architecture that require further analysis. These high risk areas are prioritized and classified for an appropriate analysis method which can range from an influence diagram in a systems dynamics model to an end-to-end test or to a fine-

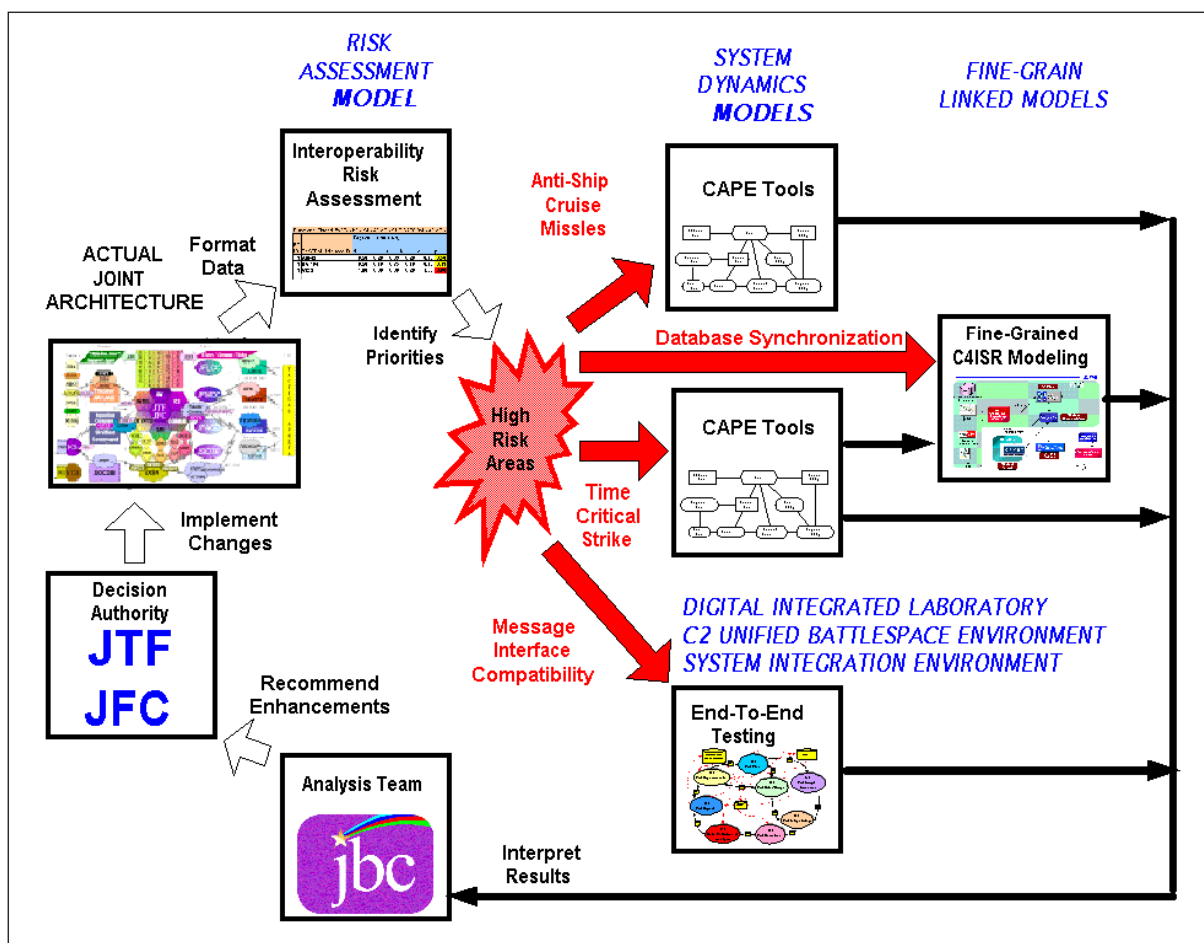


Figure 5. Risk Driven Architecture Assessment Example Showing High-Risk Areas.

grained modeling suite.

In Figure 5, there are four “high-risk” areas that show the range of architectures that could be analyzed using the JCOBIAA methodology. Each one shows the tool or combination of tools to be used for further analysis of the “high-risk” areas identified from the risk assessment tool. The first is an anti-ship cruise missile threat that could originate from the maritime phase of a combatant type JTF. After the “high-risk” area is identified using the risk assessment tool, the risk area is fed into a systems dynamics modeling tool for further analysis. The second example is related to target database synchronization, which will be analyzed using fine-grain linked models. A time critical strike risk is treated next, which is analyzed using a systems dynamic model and then is furthered analyzed using a fine-grain linked modeling tool. Finally a message interface compatibility risk is to be handled by an end-to-end test scenario tied to the functional thread used in the risk assessment. The end-to-end test will use the actual hardware and software to be fielded, only in a distributed laboratory setup such as the Joint Distributed Engineering Plant (JDEP).

3.2 Outcome Based Assessment

JCOBIAA not only focuses on identifying risk areas in the proposed architecture but is also concerned with outcome based assessment. Outcome based assessment is intended to be part of a larger outcome based interoperability process to “focus on tangible outcomes” that would be expected from the successful application of existing acquisition policies and operational tactics, techniques, and procedures (TTP). In a C4I Integration Support Activity (CISA) white paper

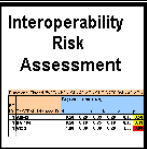
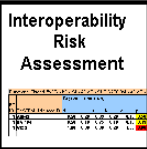

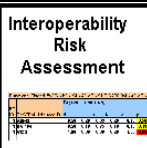

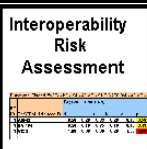
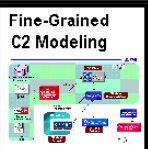
Assessment Technique	OUTCOME	
	Tangible	Contributes to
	<ul style="list-style-type: none"> Managed Risk for JTF C4ISR Architectures 	<ul style="list-style-type: none"> Full Dimensional Protection Focused Logistics Information Superiority
 	<ul style="list-style-type: none"> Reduced volume of C4ISR related problems Lower costs for JTF 	<ul style="list-style-type: none"> Focused Logistics Information Superiority
 	<ul style="list-style-type: none"> Effects based JTF planning & execution Key Insights into the relative contribution of C4ISR 	<ul style="list-style-type: none"> Precision Engagement Information Superiority
 	<ul style="list-style-type: none"> Coevolution of Mission Capability Packages 	<ul style="list-style-type: none"> Dominant Maneuver Full Dimensional Protection Focused Logistics Precision Engagement

Table 1. Assessment Techniques, Tangible Outcomes, and Contribution to JV2010.

cited by Andrews, the notion of an “interoperability value chain” is introduced to trace those outcome-bearing activities from the lifecycle of C4ISR and weapons systems to their employment by standing and contingency JTFs. [Andrews, 1998]

Table 1 lists the tangible outcomes and contribution to JV2010 mission areas for each assessment path through the risk driven example of Figure 5. The risk model alone provides an outcome of managed risk within the C4ISR architecture. This means that a documented process is being systematically applied and improved to identify high-risk areas on which to concentrate analysis and testing resources.

Tangible outcomes for combining the risk model with end-to-end testing include reduced volume of C4ISR related problems and lower costs for the JTF. Experience has shown that it costs much more to fix a problem in the field than it does in earlier stages. Tangible outcomes for combining a risk model with systems dynamics modeling include obtaining key insights on the relative contribution of C4ISR elements to the problem being considered and achieving effects based planning.

An effects based approach couples outcomes from the “execution view” to course of action selection in the “planning view.” Tangible outcomes for combining a risk model with fine-grain linked simulations include a step toward the co-evolution of mission capability packages by providing tools to facilitate the “melding of a concept of operations, C2, organization, doctrine, weapons and infrastructure, systems and personnel” into a coherent military force. [Alberts *et al.*, 1999]

3.3 Functional Threads

A functional thread can be thought of as a series of tasks that when completed constitute a desired outcome. They also serve as a bridge between the organization and system views of an architecture to focus the analysis and test efforts on capabilities rather than systems. The power of functional threads can be illustrated in an example from the design of complex circuit card assemblies. The function of this circuit card was to connect six independent radio circuits with a digital telephone-switching matrix. The card had numerous surface mounted components and required a mezzanine board to handle all of the voice and control signals required by the radios. Figure 6 shows a simplified functional block diagram for the radio circuit card. The traditional approach could take a month to verify the initial prototype based on similar boards developed for this project. Each section of the circuit card would be populated with components and tested before proceeding to the next section. Several weeks could elapse before the last section was tested and the circuit card was deemed operational.

A non-traditional approach was used in developing the circuit card in an attempt to decrease the testing time. The strategy was to populate the entire board and use a *functional thread* of radio audio to test the circuitry. The idea was to insert an audio tone at the input of radio port 6, have the switching matrix (not shown) connect the audio to the output of radio port 1 following the highlighted path in Figure 7.

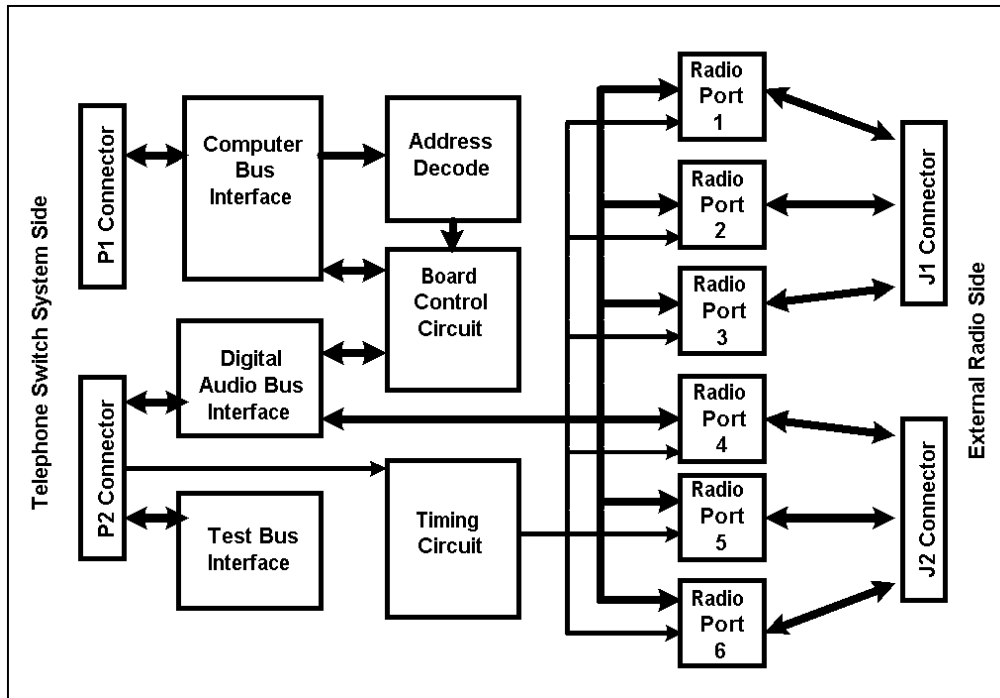


Figure 6. Radio Circuit Simplified Functional Block Diagram.

Once the test was set up, if a tone could heard coming from radio port 1 then the majority of the circuitry *had to be functioning correctly*. The end result was that by leveraging the idea of a functional thread the radio interface module was deemed operational in less than a week, thus reducing the testing time by 75%. This example shows how functional threads can be used to

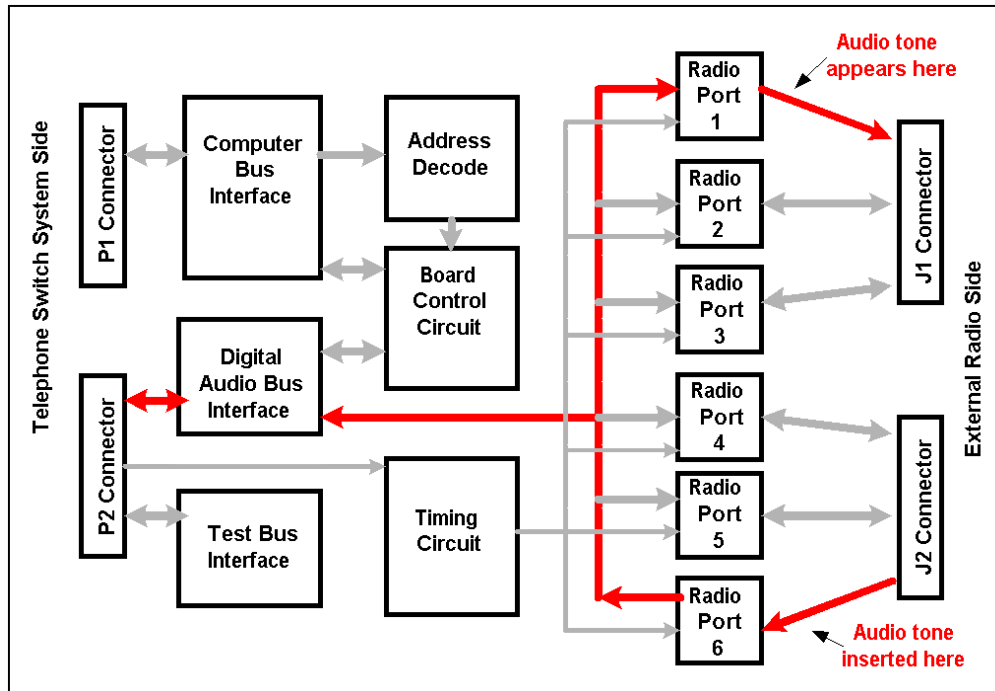


Figure 7. Audio Loop Back Test as a Functional Thread Example.

not only functionally test the proposed architecture but to test it from a systems point of view and save time and money in the process. The JCOBIAA methodology is proposing to use functional threads in the same way but on a broader scale.

In the case of the JTF commander, functional threads will be taken from Joint Vision 2010 (JV2010) mission areas as shown in Figure 8. The Joint Vision 2010 mission areas include:

- Information Superiority
- Dominant Maneuver
- Power Projection
- Full Dimensional Protection
- Regional Engagement and Presence
- Force development requirements, and readiness
- Logistics, Sustainment, and Support
- Intelligence, Surveillance, and Reconnaissance (RECCE)
- Special Warfare and Special Access

Some examples of Navy High Level Functional Areas (HLFA) flowing down from the JV2010 mission areas are shown in Figure 9. Within the Command and Control (C2) Weapons Control there are essential fleet capabilities. These essential fleet capabilities become functional threads when they get mapped into equipment strings that can be exercised to realize the capability.

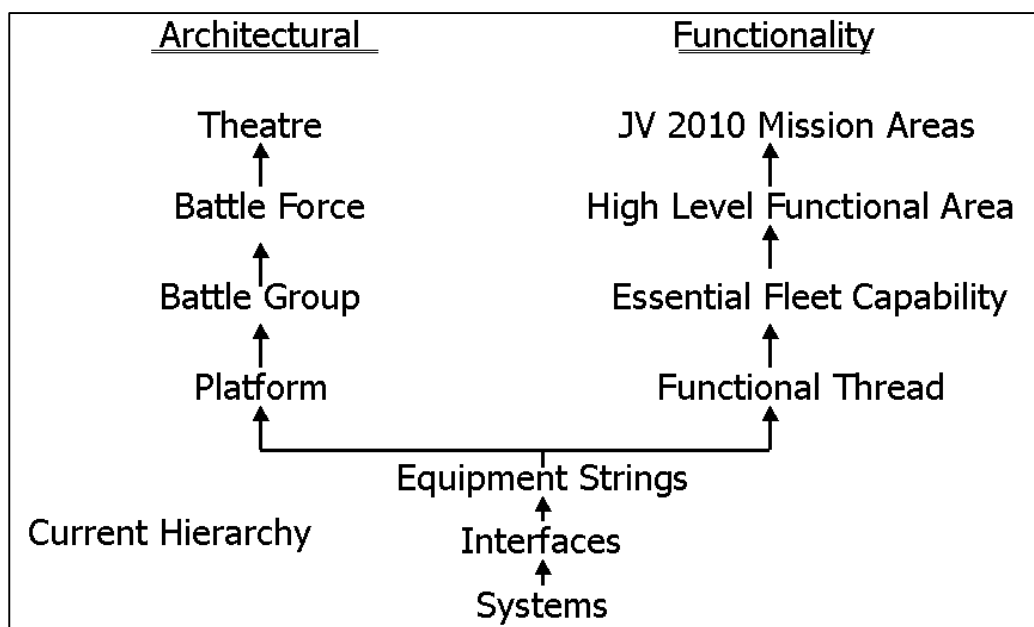


Figure 8. Relationship of Functional Threads to JV2010 Mission Areas and Systems.

The JV2010 mission areas form the basis for the Navy's High Level Functional Areas (HLFA). Some examples of the Navy High Level Functional Areas (HLFA) that flow from the JV2010 mission areas are shown in Figure 9.

Navy Example High Level Functional Areas to be End-End Tested

- | | |
|-----------------------------|---------------------------------|
| • Allied Interoperability | • Logistics |
| • C2 Force Control | • NVI End-to-end Infrastructure |
| • C2 Force Coordination | • RECCE |
| • C2 Weapons Control | • Space & Electronic Warfare |
| • Deterrence | • Special Warfare |
| • Electronic Navigation | • Strategic Mobility |
| • Environmental Security | • Strike Warfare |
| • Information Warfare | • Surveillance |
| • Intelligence | |
| • Joint Interoperability | |

Figure 9. High Level Functional Area Examples

Within the Command and Control (C2) Weapons Control HLFA there are numerous essential fleet capabilities. These essential fleet capabilities (Figure 10) become functional threads when they get mapped into equipment strings that can be exercised to realize the capability.

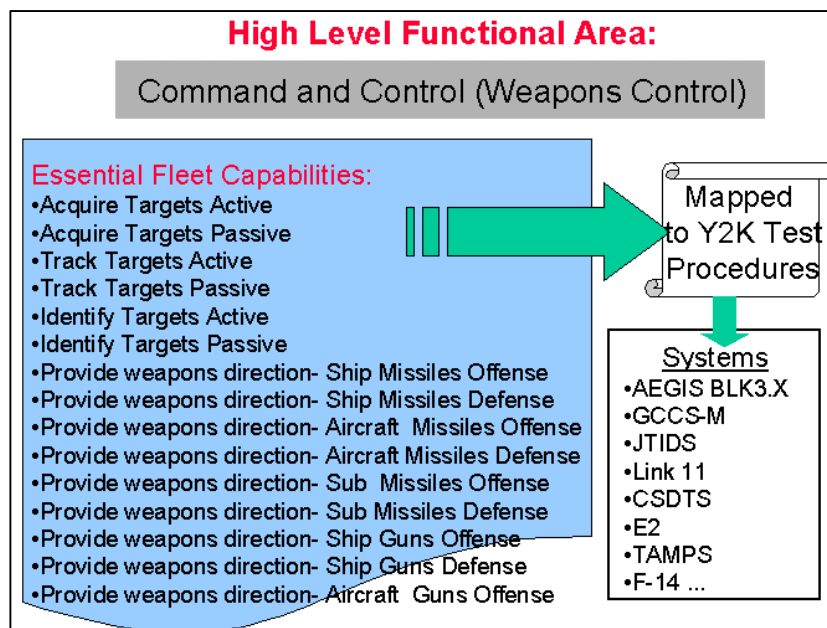


Figure 10. Example of Functional Thread Mapping for Y2K Test Procedure.

Functional threads are not exhaustive representations of all physical implementation or equipment strings that could be realized to enable the desired capability. A functional thread follows one possible path of communications and does not impose parallel or redundant path requirements. [SSC-C, 2000]

The Navy has done additional work in the area of analysis of functional threads that serves as a basis for continued development and provides potential tools to build upon. In particular, the JMTIRA tool that was developed for the Y2K testing proved that traceability from JV2010 mission areas to functional threads to systems was possible (Figure 8).

3.4 Architecture Assessment Tools

The JCOBIAA study team is looking at various tools to assess JTF architectures. For the risk assessment model, the JMTIRA tool developed by the Navy for their Y2K testing is the initial choice. System dynamics modeling tools using influence diagrams provide a high level way to evaluate the JTF architecture and include MITRE's C4ISR Analytic Performance Evaluation (CAPE) models, SAIC's Situation Influence Analysis Module (SIAM), and the Air Force Research Laboratory (AFRL) Rome Lab's Campaign Assessment Tool (CAT). Fine-grain linked modeling suites using linked simulations provide a more detailed analysis of the JTF architecture and include MITRE's Multi-Tier Simulation of Executable Architecture Views (MSEAV) and George Mason University's Computer Aided Evaluation of Systems Architectures (CAESAR II) tools. [Pawlowski, 1999]. End-to-End testing is used for actual hardware and software connections for a definitive understanding of system performance and problems. The process and environments used for end-to-end testing include the Joint Distributed Engineering Plant (JDEP) resources of the U. S. Army's Digital Integrated Lab (DIL), the U.S. Air Force's C2 Unified Battlespace Environment (CUBE), and the U.S. Navy's Systems Integration Environment (SIE).

3.5 Risk Assessment Model

The risk assessment model is based on leveraging the success of JMTIRA. JMTIRA was developed for the Navy's Year 2000 (Y2K) End-To-End (ETE) C4ISR testing process. With 240 systems to test and a vast number of possibilities for interconnecting them, a method for prioritizing the test effort was needed. The method calculates risk factors of functional threads representing the probability of failures in the ETE architecture for essential fleet capabilities. The components of risk that weigh into the process include system characteristics, fleet criticality, and ETE testing & history (Figure 11).

When the calculated engineering risk factors of systems were plotted against reported fleet issues, high-risk assessment scores were found to be consistent with the historical trend in fleet reported issues. Fleet issues are an outcome based measure in themselves and reducing them increases interoperability that leads to information superiority.

As a prefiltering mechanism for C2 assessment, JMTIRA would be adapted for analyzing JTF architectures. Alternatively, a tool like the Joint Operations Tactical Interoperability Database

(JOTID) being developed by the Logistics Management Institute for NATO NC3A could be adapted for the same role.

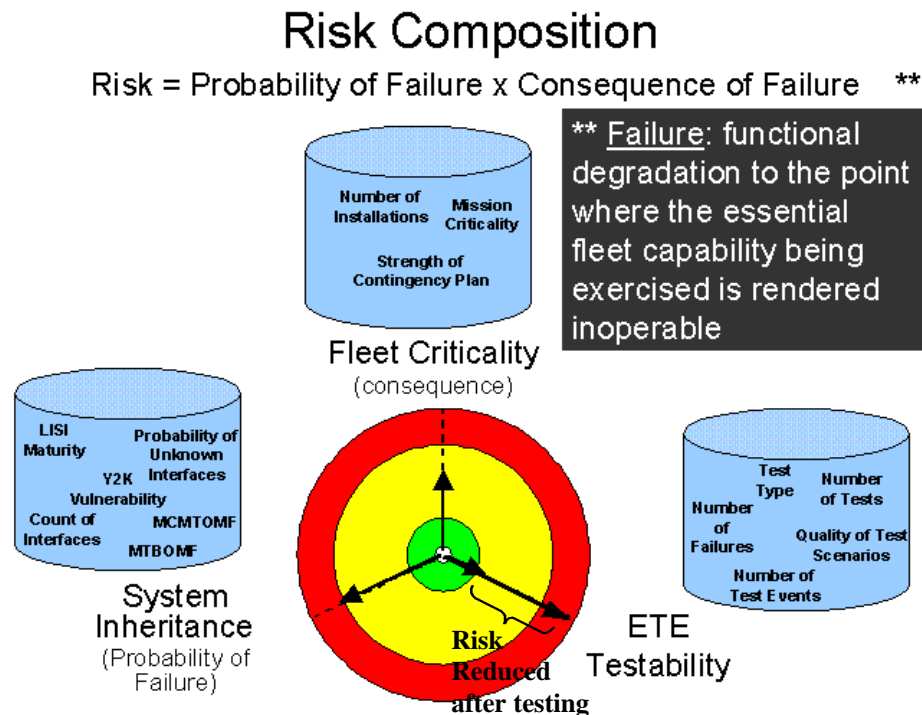


Figure 11. Risk Composition Used in JMTIRA Process.

The formulas used in calculating risk for functional threads have been evolving by incorporating feedback in the form of experience data from testing and force deployments. Initial formulas were based on the characteristics thought to influence risk. These formulations provided a starting point, but they are subjective in nature.

Y2K testing provided JMTIRA with a data set to use in shaping the risk ranking scores into more interpretable and statistically sound risk measures. Regression analysis was applied to determine what characteristics significantly impacted the performance of systems in end-to-end testing and to provide a better model for predicting the probability of failure.

For example, data from five deploying battlegroups were analyzed to reveal that adding one interface to any system results in a 1.5% increase in the chance of a failure. A system categorized as “connected” under the Level of Information Systems Interoperability (LISI) showed a five-fold increase in the chance of failure compared to the systems with other LISI categories. Non-mission critical systems were 26 more times likely to experience a failure than mission critical systems. [CAWG, 1998][SSC-C, 2000]

There is a need to extend the risk assessment methodology beyond interoperability issues to other dimensions that relate to outcomes. For example, formulas for the information security of

functional threads could be developed and the risk model needs to account for JTF activities like those contained in the Unified Joint Task List (UJTL).

The JMTIRA risk model can be considered to be “capability driven.” It uses a hierarchical linkage from the JV2010 mission areas to equipment strings that instantiate functional threads. See Figure 12. The influence of threats is not considered and the operational force information is limited to equipment types and software versions of the components that make up the equipment strings.

The example shows an equipment string selected from a functional thread related to the “acquire targets active” essential force capability. Risk factors for the interface, R_I , system, R_S , and functional thread, R_{FT} , are depicted in Figure 12.

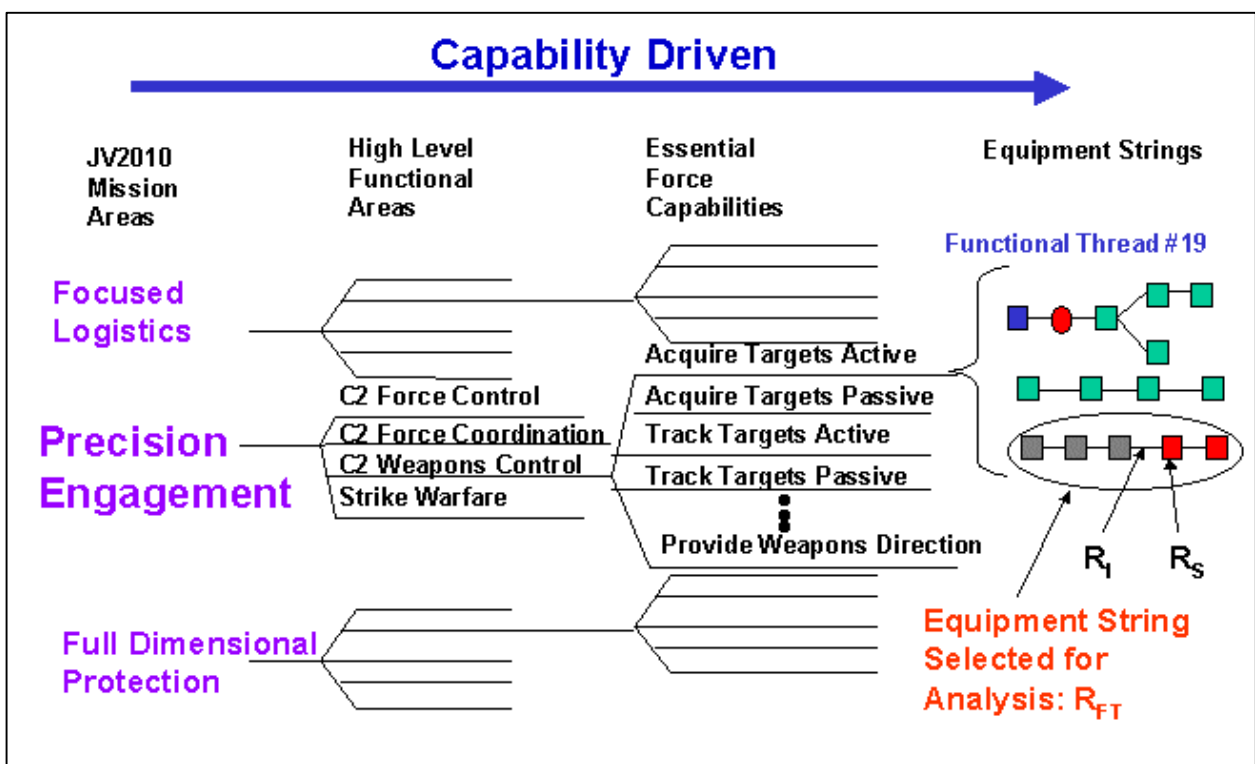


Figure 12. Capability Driven Risk Model Showing Hierarchical Relationships.

One way of extending JMTIRA’s capability driven risk model is to add a “threat driven” risk model component that includes both the UJTLLs and threats. The form of such a risk model is shown pictorially in Figure 13. A threat model and an operational model are used to build influence diagrams of mission threads relevant to the JTF under consideration. These mission threads are related to the UJTL technical tasks which, in turn, are related to functional threads. These functional threads are used to select equipment strings as in the capability driven risk model discussed earlier.

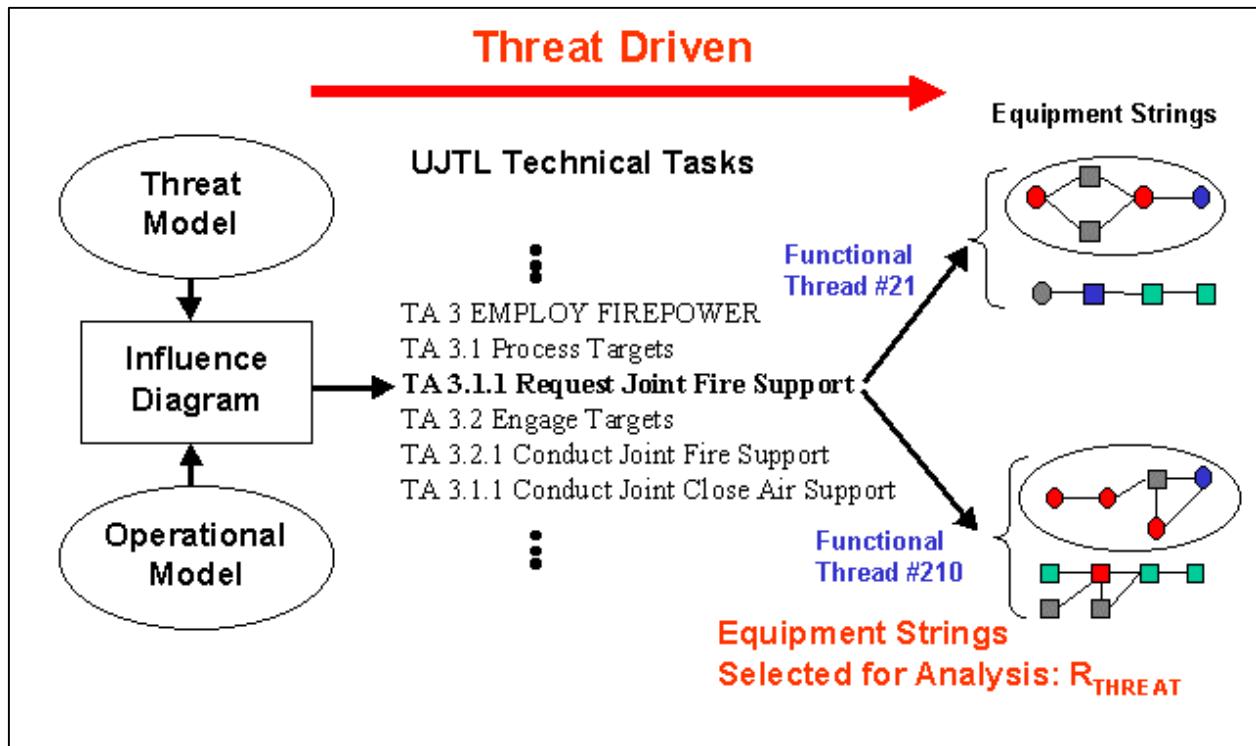


Figure 13. Threat Driven Risk Model Showing Relationships to UJTLs.

In the example shown, an influence diagram (not shown in detail) has been used to evaluate a mission thread related to the UJTL technical task “TA 3.1.1 Request Joint Fire Support.” This task is related to two functional threads, numbers 21 and 210. Each of these functional threads could be realized by two different equipment strings. One equipment string from each group is selected for analysis and a threat risk, R_{THREAT} , is calculated.

The mission threads with high-risk scores can then be analyzed further. For example, when followed by analysis with a CAPE model a high-risk area can be explored in greater detail to gain insights into what values are appropriate for the metrics associated with each task from the UJTL.

In the JCOBIAA risk model depicted in Figure 14, the capability and threat driven components are used together. In the combined example, an equipment string associated with the “Acquire Targets Active” is identified as a “high-risk for capability.” What is the threat implication for this high-risk capability? Since its functional thread can be related to the UJTL “3.2 Engage Targets,” an influence diagram can be used to provide insights to this question.

Also in the example, an equipment string associated with the UJTL “TA 3.1.1 Request Joint Fire Support” is identified as a “high-risk for threat.” What is the capability implication for this high-risk threat? Interface, system, and functional thread risk factors can be calculated for this equipment string to help answer this question.

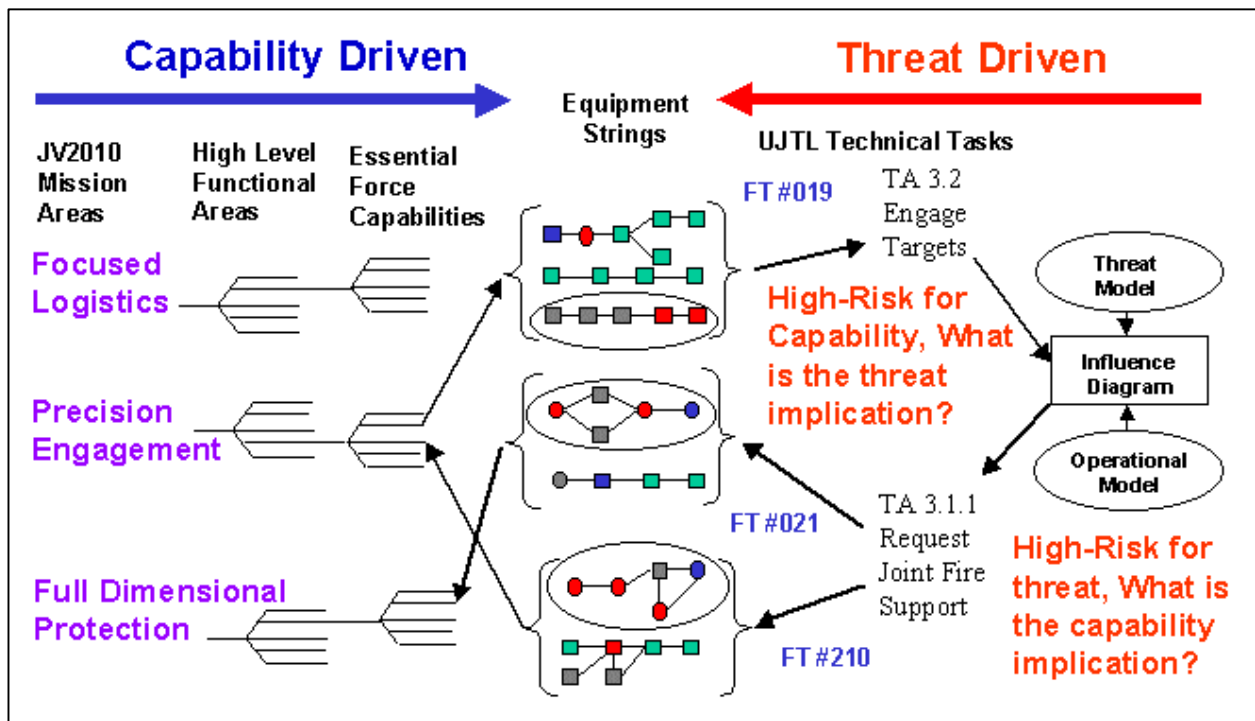


Figure 14. JCOBIAA Risk Model Showing Capability and Threat Driven Components.

Equipment strings that appear as high-risk from both the capability and threat perspectives would merit special attention.

In addition to their role in the threat driven component of the JCOBIAA risk model, influence diagrams also play a role in probing deeper into problem areas that have been identified in the risk model.

3.6 Influence Diagrams and System Dynamics Models

Influence diagrams provides a graphical “open box” way to achieve a shared understanding of the problem, issues, and implications. System Dynamics Models use a probabilistic approach in analytic uncertainty analysis as opposed to the stochastic approach used in discrete event simulation models to provide insights into and analysis of the architecture (Figure 15). Both of these methods give results at a high level but in less time than results from a simulation model would take to generate. This makes them ideal for analysis that has to be done in a very short period of time. [Morgan and Henrion, 1990]

One outcome of this analysis is an “architecture driven” choice of tactics. This type of analysis is not intended to predict exact outcomes. It is a tool to gain insights into the relative contributions of C4ISR to prosecuting the mission. Hughes describes how the “salvo equations” can be used to understand the dynamics of modern missile combat. [Hughes, 2000]

One of the tools being considered for the system dynamics model is the CAPE models which have been developed by Henry Neimeier of MITRE. Neimeier followed a similar line of thought to Hughes with his process for modeling the precision strike process using a CAPE model. [Neimeier, 1996]

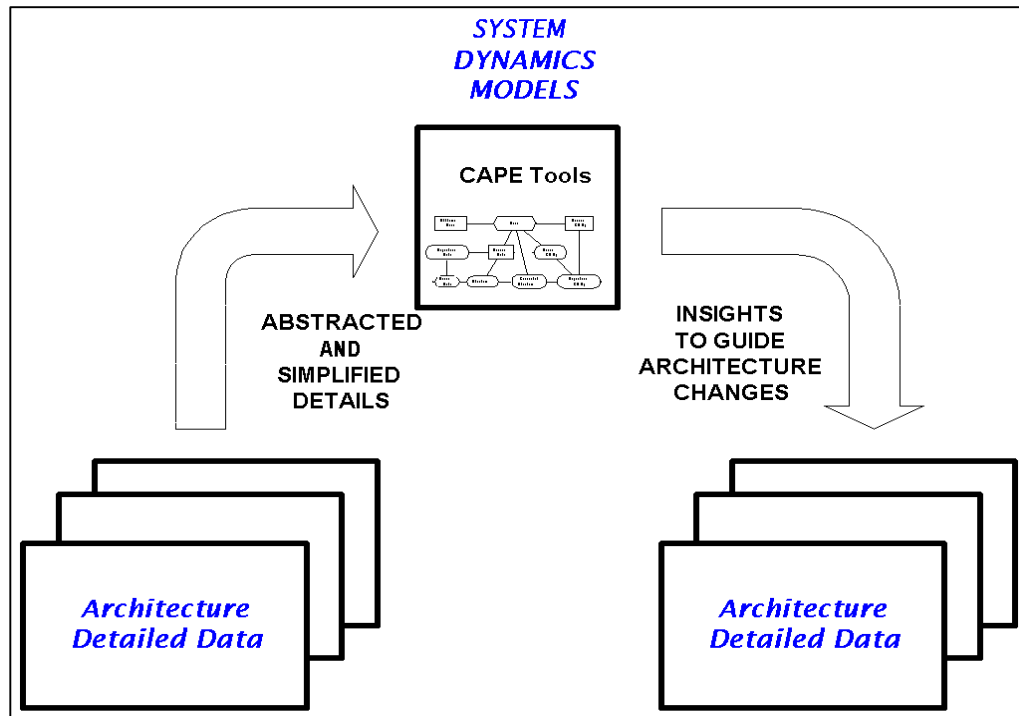


Figure 15. Abstracting Architecture Details to Provide Results from Simplified Analytical Models.

Some areas of risk within the architecture may best be suited for this type of analysis. Examples include understanding the threat posed by anti-ship cruise missiles or the ability to strike time critical targets (Figure 5). Due to the dynamic interactions between different architectures posed in both of these examples, system dynamics models handle this interaction well.

Although both of these examples provide insights into dynamics, for JTF architecture assessment the maximum utility in identifying relevant problem areas and potential solutions is achieved when the influence nets and parameter values are abstracted from the architecture details. These details could be pulled from the databases used to feed the risk model to provide better results.

One caution in using these high level simplified models is that the models need to be empirically validated to insure the insights they provide are relevant and not misleading. [Morgan and Henrion, 1990]

3.7 Fine-Grain Linked Models

JCOBIAA is considering two fine-grain linked models for use in the methodology when the system dynamics tools do not provide enough detail and when end-to-end testing is impractical. One such tool is the Multi-Tier Simulation of Executable Architecture Views (MSEAV) that is

being developed by MITRE for the US Army to provide a capability for assessing integrated architectures in terms of measures of performance and effectiveness. MSEAV has made progress establishing relationships between operational architecture and system architecture models. MSEAV is built from Commercial Off-the-Shelf (COTS) products ranging from business process reengineering tools for modeling operational views to OPNET for rigorous modeling of underlying communication networks.

The other fine-grain modeling tool, Computer Aided Evaluation of Systems Architectures (CAESAR II), uses linked petri net models to study the behavior of information architectures. The latest version is web based and uses a graphical interface to drive simulations for effects based planning. Analysts use influence net models to evaluate different courses of action. Tasks are converted into actionable events in the form of executable petri nets in the Design/CPN software package that users access through a web interface.

3.8 End-to-End Testing

End-to-End testing is useful to test functional threads with actual equipment strings before they are deployed in the field. This type of testing has been successfully performed for Year 2000 (Y2K) testing and more recently for System Performance & Interoperability Testing (SPIT) at SSC-C. The Systems Integration Environment (SIE) test process used by the U.S. Navy is depicted in Figure 16. By using a common process with common tools a great deal of

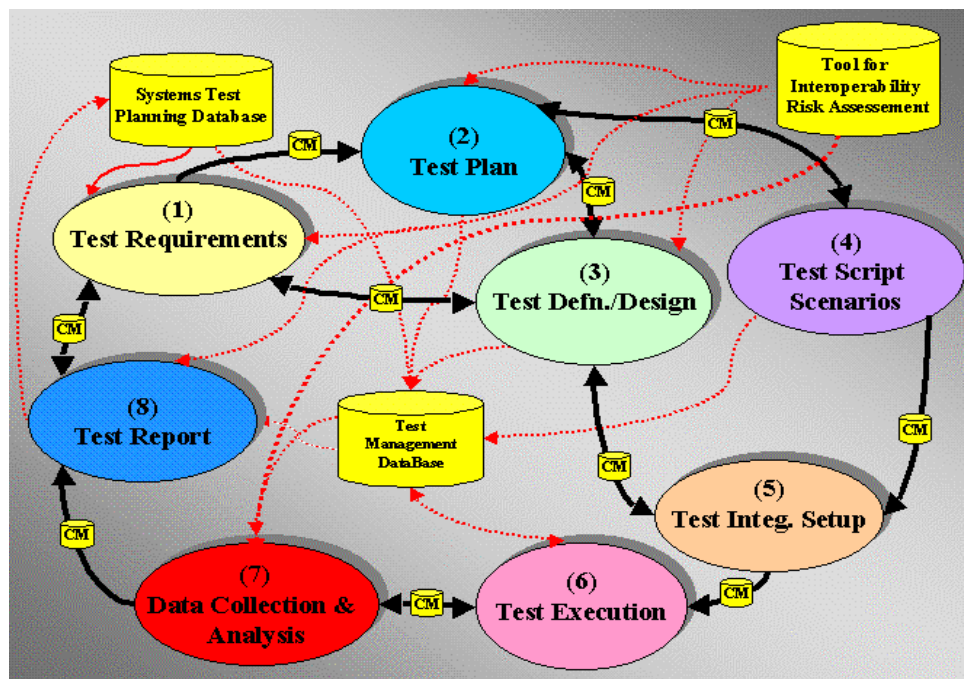


Figure 16. Systems Integration Environment Test Process.

consistency and reuse of test resources and knowledge is achieved. Each step in the process is connected with the others though Configuration Management (CM). Discipline is exercised so that all new requirements and test configurations become part of the CM process or they are not

allowed to be used for testing. A Test Management Database (TMDB) is used to manage the test related information at every step.

The test requirements are established from sources including user input, previous test results, data collection plan, system interface mapping, system to function matrix, and systems test planning database.

An example end to end test configuration used for the USS Constellation Battlegroup Y2K testing is shown in Figure 17. The interface risk factors are depicted in red, yellow, and green for a partial test architecture for four functional threads involving ship-ship-shore connectivity. A number of different labs and test facilities are connected together for the test. System configurations and software versions for various platforms are replicated in the lab to provide the realism of the fielded systems in a controlled environment.

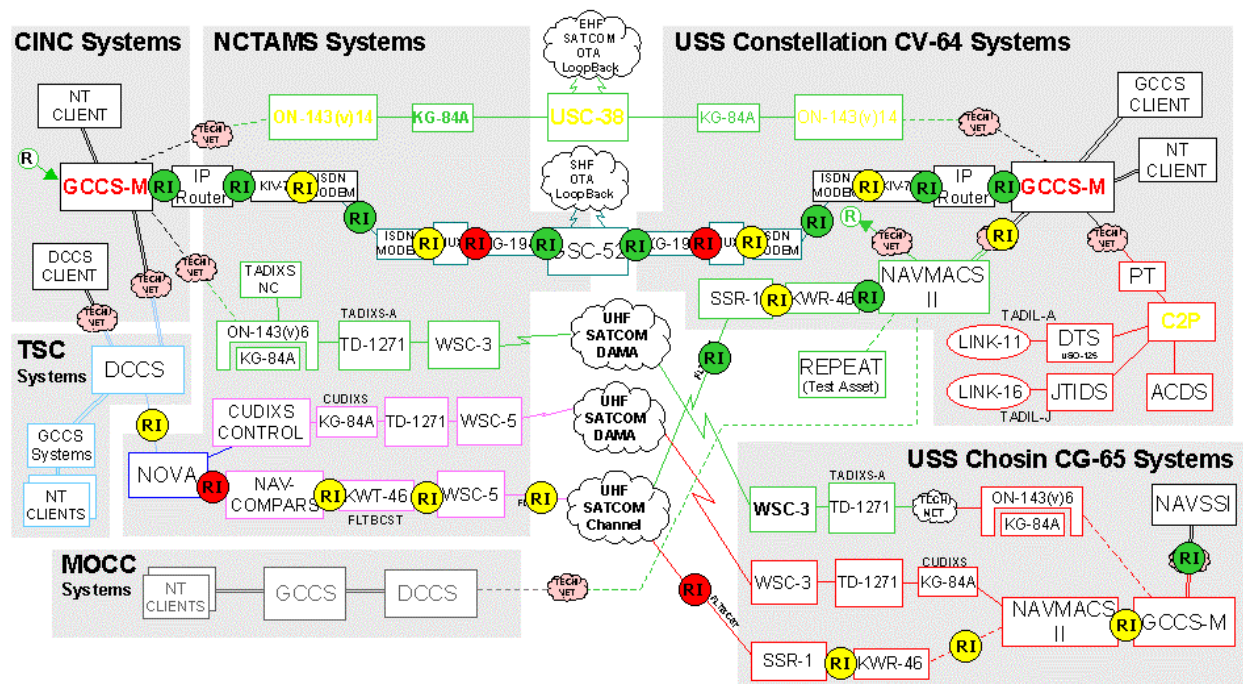


Figure 17. Example of End-To-End Test for Used for Y2K Testing.

End-to-end testing for functional threads of JTF architectures could be accomplished using the Joint Distributed Engineering Plant (JDEP) concept and resources. Just as the Navy has developed their SIE process, the Army has developed its Digital Integrated Laboratory (DIL) and the Air Force its C2 Unified Battlespace Environment (CUBE). See Figure 18.

These lab capabilities will form the building blocks for JDEP. JDEP is an assembly of existing combat systems engineering sites interconnected via emulated tactical data links stimulated in a synchronized fashion. The JDEP replicates the joint forces battlefield scenario in a controlled environment. It provides the capability to address joint service system performance in a system of systems environment and include command and control elements as part of the test environment.

The JDEP will initially focus on air defense, but the concept supports testing for other aspects of the JTF architecture.

The JDEP shares some of the same goals as JCOBIAA. Namely, to identify issues before deployment. Additionally, by conducting the tests in a controlled environment, joint operation issues to be framed so that they can be dealt with through changes in TTP or engineering solutions.

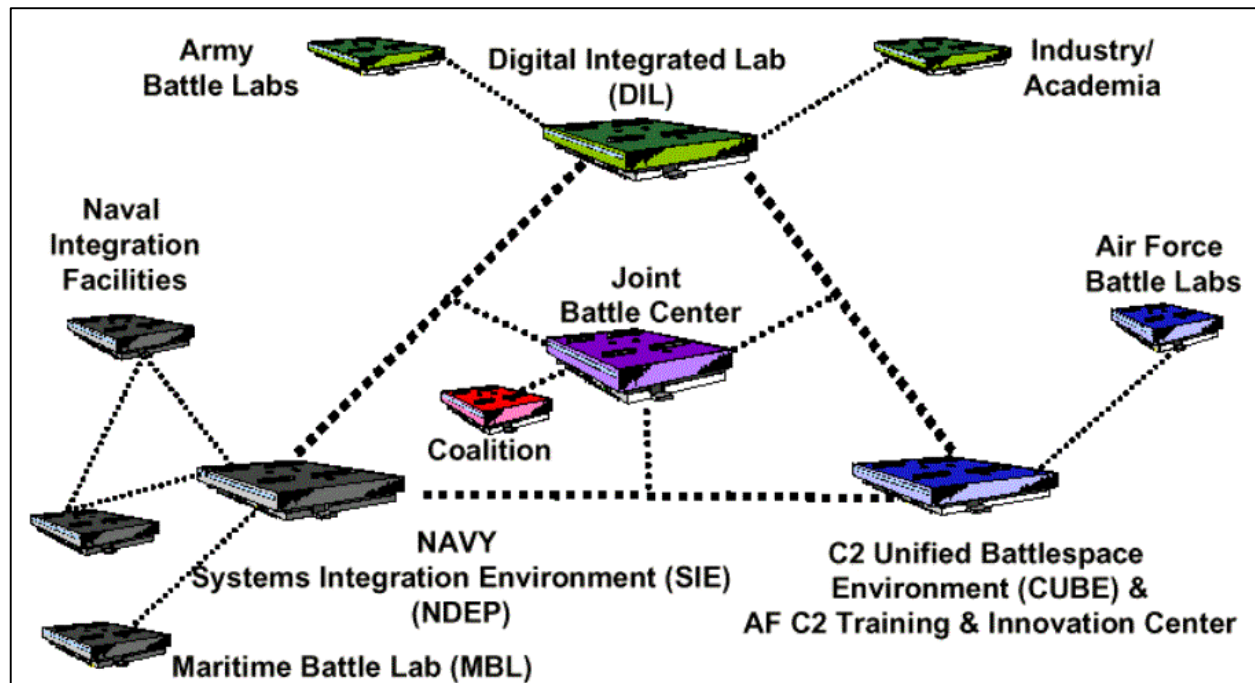


Figure 18. Joint Distributed Engineering Plant for End-To-End Testing of JTF Functional Threads.

4. Conclusion

This paper has outlined a risk driven outcome based integrated architecture assessment methodology that the JCOBIAA study team is developing at the Joint C4ISR Battle Center. The goal is an assessment methodology that can be used to get results quickly as a JTF is forming. This technique builds on the NATO Code of Best Practice for C2 Assessment by adding risk assessment as a mechanism for narrowing the scope of the architecture that needs to be analyzed or tested. The objective is to surface deficiencies in the architecture and to identify potential fixes before problems arise in the field.

The team's study of architecture assessment has confirmed that there is no single tool which can provide a total assessment. This is why the emerging JCOBIAA methodology includes multiple tools.

There are several challenges to overcome in the team's quest for an efficient architecture assessment methodology. These include:

- Efficient ways of federating the relational databases containing the system and equipment configuration information needed to feed the risk model
- Efficient mechanisms for abstracting simplified, yet meaningful, models from the integrated architecture information
- Mechanisms for translating the results of analysis and testing into enhancements to the JTF architecture
- Process that allows rapid set-up and execution of ETE testing of JTF functional threads
- Making the assessment methodology easy to use and understand

The strategy for overcoming these hurdles is based on leveraging several on-going initiatives. Following a defined systems engineering process and intelligent reuse of proven practices are key elements of the team's plan. Near term efforts include identifying changes required in JMTIRA for interoperability risk assessment of JTF architectures, identifying strategies for obtaining appropriate "slices" of operational architectures for fine-grained modeling, and formalizing the overall assessment methodology including sensitivity analysis & Verification, Validation, and Accreditation.

These near term efforts will need to be accomplished before the JCOBIAA architecture methodology is complete. This methodology offers an opportunity for C4ISR architecture assessment that may prove valuable to solving JTF commander's immediate and most critical problem of assembling disparate organizations and their underlying infrastructures to form an effective fighting force.

5. References

[Alberts *et al.*, 1999] David S. Alberts, John J. Garstka, Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition (Revised), DoD Cooperative Research Program, Washington, DC., August 1999.

[Andrews, 1998] Duane P. Andrews, *A Recommended Blueprint for the ASD(C3I) and CIO in response to Defense Reform Initiative #17: An Outcome Based Interoperability Improvement Process for the DoD*, March 11, 1998. Available at <http://www.fas.org/irp/doddir/dod/blueprint.html>

[CAWG, 1997] C4ISR Architecture Working Group, *C4ISR Architecture Framework*, Version 2.0, 18 December 1997.

[CAWG, 1998] C4ISR Architecture Working Group, *Levels of Information Systems Interoperability (LISI)*, 30 March 1998.

[Ellis, 1999] Admiral James O. Ellis, U.S. Navy, *A View from the Top*, Observations from the Commander, Joint Task Force NOBLE ANVIL during Operation ALLIED FORCE, July 1999.

[Hughes, 2000] CAPT Wayne R. Hughes Jr., USN (Ret), *Fleet Tactics and Coastal Combat*, 2nd Ed., Naval Institute Press, Annapolis, MD, 2000.

[JCS, 1995] Joint Chiefs of Staff, *Unified Action Armed Forces (UNAAF)*, Joint Pub 0-2, 24 February 1995.

[JCS, 1997] Joint Chiefs of Staff, *Joint Doctrine Capstone and Keystone Primer*, 15 July 1997.

[Levis, 2000] Alexander H. Levis and Lee W. Wagenhals, *C4ISR Architecture Framework Implementation*, AFCEA Coursebook 503J, February 8-11, 2000, San Diego, California.

[Morgan and Henrion, 1990] M. Granger Morgan and Max Henrion, *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*, Cambridge University Press, New York, NY, 1990.

[Neimeier, 1996] Henry Neimeier, *A New Paradigm for Modeling the Precision Strike Process (U)*, IEEE Military Communications Conference (MILCOM), 1996.

[NATO, 1998] Research Study Group on Modelling of Command and Control (C2), *Code of Best Practice*, NATO Panel 7, Technical Report AC/243(Panel 7) TR8, 1998 Edition.

[Pawlowski, 1999], Dr. Mike Hamrick, and Steve Ring, *Multi-Tier Simulation of Executable Architecture Views*, The MITRE Corporation, 1999.

[SSC-C, 2000] Spawar Systems Center Charleston/Science Research Corporation, *Interoperability Risk Analysis Technical Whitepaper on Approach and Implementation*, Draft Working Paper.

[Starr, 1998] Stuart H. Starr, *Evaluating the Impact of C3I on Mission Effectiveness*, Proceedings of the Fourth International Symposium on Command & Control Research & Technology, Nasby Slott, Sweden, September 14-16, 1998.